PracticalAdvice
From the Corporate Department

Fox Rothschild LLP
ATTORNEYS AT LAW

Cybersecurity: A Concern for Every Business

Cybersecurity. It may sound like a Hollywood hook for the futuristic "I Robot" movie genre, but as the recent data breach at Target has shown us, it is most definitely an issue for today. Recent reports emphasize that any business that relies on individual, proprietary and/or customer data (which by definition includes every business) is at some level of risk of being a victim of "cybercrime" conducted through Internet-based attacks on an enterprise's information technology systems.

The potential costs to a victimized business are varied (and perhaps not so obvious on first blush):

- Investors may question whether directors and management have fulfilled their fiduciary and statutory duties to protect the company's key assets.
- Unhappy employees may disclose sensitive data.
- Competitors may gain access to trade secrets.
- Exposure of sensitive personal information may be fodder for the class action bar.
- Federal and state governmental authorities may seek to assess penalties for failure to comply with laws requiring reporting of suspected breaches involving such data.

The role of the business lawyer in such circumstances is to first educate the company's directors and managers as to the legal risks and then help the company formulate a comprehensive approach to identifying vulnerabilities within its structure, implementing measures to minimize the risk of cybercrime and, recognizing that the bad actors are moving at a speed faster than the programmers can formulate responses, mitigating the damage suffered in the event of a breach. This is, by necessity, a cross-disciplinary process, as it calls into play company personnel and third-party professionals (both legal and non-legal) from such areas as information technology, human resources, business development, supply chain management, investor and government relations, crisis management and insurance.

Companies must recognize the reality of the situation that a breach may not become apparent until long after it has occurred. Consequently, the dual challenge is to design and implement strategies to prevent data breaches and simultaneously develop a plan to contain, to the extent practicable, the damages and liabilities for data related losses.

Company counsel must be vigilant in advising that appropriate attention be afforded to cybersecurity issues on a regular basis as an element of sound corporate practice. Such a focused approach should produce not only the short-term benefit of decreasing the likelihood of a breach but also serve as the cornerstone to defenses against claims that the company did not take adequate steps to protect the security of its data. This should further contribute to the enterprise's long-term liquidity value as prospective investors in and/or purchasers of the business must be expected, as a matter of standard due diligence, to pose questions regarding the elements of the company's cybersecurity programs, how the company has structured its vendor agreements to allocate responsibility for safeguarding systems and data, whether any breaches have occurred that may undermine the value of the company's key intellectual property or other assets and what actions may be pending or threatened arising out of cybersecurity incidents.

For more information, please contact:

Michael P. Weiner, Esq.
609.844.3032
mweiner@foxrothschild.com

Copyright © 2014 Fox Rothschild LLP | Attorney Advertising

California | Colorado | Connecticut | Delaware | District of Columbia | Florida | Nevada | New Jersey | New York | Pennsylvania